UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/974,705 | 10/10/2001 | Marco Macchetti | 01AG17653537 | 7872 |

27975 7590 06/28/2005

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

| EXAMINER | |
|---|---|
| COLIN, CARL G | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/974,705 | MACCHETTI ET AL. | |
| | Examiner | Art Unit | |
| | Carl Colin | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *17 April 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *21-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 April 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

## DETAILED ACTION

1. In response to communications filed on 4/17/2002, applicant cancels claims 1-20, and adds claims 21-47. The following claims 21-47 are presented for examination.

### *Specification*

2. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code on pages 1-2. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

### *Claim Rejections - 35 USC § 112*

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 25 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3.1 Regarding claim 25 the recitation "wherein performing comprises performing at least one transformation round once a non-transposed state array in at least one of the plurality of transformation rounds" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by " performing at least one transformation round once a non-transposed state array "), thereby rendering the scope of the claim(s) unascertainable.

*Claim Rejections - 35 USC § 103*

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 21-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2001/0024502 to **Ohkuma et al**.

4.2 **As per claims 21, 26, 31, and 44, Ohkuma et al** substantially teaches a device for converting data between an unencrypted format and an encrypted format, the device comprising: at least one register for storing the data in the form of bit words (see figure 10); and a circuit for performing a plurality of transformation rounds, each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array (page 12, paragraphs 261-274), and **Ohkuma et al** discloses transposing rows and columns of the state array to form a higher level matrix that meets the recitation of a transposed state array and further discloses using such matrix for executing a transformation (page 12,

paragraphs 268-273) that meets the recitation of transposing rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array. **Ohkuma et al** in another embodiment discloses applying key scheduling on a higher level MDS matrix, for example (page 13, paragraphs 306-315). Although **Ohkuma et al** does not disclose the same architecture as in applicant's disclosure, **Ohkuma et al** discloses different arrangements in the disclosure that read on the claimed language as claimed and any combination or omission of some of the components of exemplified arrangement or any other arrangement disclosed in **Ohkuma et al**'s would require routine skill in the art and therefore, would be an obvious modification to one skilled in the art to reach a design goal (page 15, paragraphs 352-354).

**As per claims 22** and **32**, **Ohkuma et al** discloses the limitation of wherein said at least one register stores bit words as 8-bit words (page 6, paragraph 128).

**As per claims 23** and **33**, **Ohkuma et al** discloses the limitation of wherein said circuit operates on a state array comprising a 4x4 matrix of bit words (page 6, paragraph 128).

**As per claims 24** and **34**, **Ohkuma et al** discloses the limitation of said circuit in performing a plurality of transformation rounds performs at least 10 transformation rounds (page 4, paragraph 92).

**As per claim 25**, **Ohkuma et al** does not explicitly disclose the claimed language of claim 25 as claimed. Examiner will interpret the claim to disclose that one of the rounds to be bypassed as shown in prior art figure 4 of Applicant's disclosure. Therefore, having at least one round performed on a non-transposed state is well known as disclosed in Rijndael cipher algorithm. (See also page 13, paragraph 305).

**As per claim 27**, **Ohkuma et al** discloses the limitation of wherein the at least one round key is transposed (see figure 3 and figure 6 and page 5, paragraph 109).

**As per claims 28-30**, **Ohkuma et al** discloses the limitation of adding code to transpose the at least one round key wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round key schedule wherein the round key schedule comprises a transposed round key schedule (pages 4-5, paragraphs 90-98 and page 5, paragraph 109).

**As per claims 35-36,** and **45**, **Ohkuma et al** discloses that the invention can be performed by any number of modules and any combination of bits that meets the recitation of wherein said circuit comprises at least one S-box processing module, said at least one S-box processing module operating on a group of bit words defining a cell of a column of the state array and each of the plurality of S-box modules operating on a corresponding cell of a column of the state array (page 3, paragraphs 62-65).

**As per claim 37**, **Ohkuma et al** discloses the limitation of wherein the column of the state array comprises four cells (page 4, paragraph 92).

**As per claims 38-39** and **46-47**, **Ohkuma et al** discloses that the invention can be performed by any number of modules and any combination of bits wherein the circuit further comprises a plurality of shift column modules, (page 3, paragraphs 62-65); and further discloses shift up can be performed (page 5, paragraph 117); column mix is also a well known process as disclosed in Rijndael cipher algorithm (page 1, paragraph 5 and page 4, paragraph 87) that meets the recitation of each of said plurality of shift column modules to perform a column shift operation on a column of the state array and the limitation of wherein a column shift operation performed by each of said plurality of shift column modules generates shift column data, and wherein said circuit further comprises a single mix column module to perform column mix operations on shift column data

**As per claims 40-43**, **Ohkuma et al** discloses an encryption and decryption apparatus that meets the recitation of encoder for converting data from an unencrypted data format to an encrypted data format and a decoder for converting data from an encrypted data format to an unencrypted data format (page 15, paragraph 343-349). **Ohkuma et al** further discloses an encryption and decryption apparatus formed as a semiconductor device that meets the recitation of embedded system for use in a smart card (page 15, paragraph 343-349).

*Conclusion*

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses Rijndael cipher algorithm and variations and discloses algorithms with permutation of rows and columns.

US Patent Publication: US 2002/0157009 Yamamoto et al; US 2002/0191784 Yup et al.

US Patents: 5,533,127 Luther.

Non-Patent Literatures: Mc Loone, Maire; McCanny, John V; "Rijndael FPGA Implementation Utilizing Look-Up Tables"; 26-28 Sept. 2001; Signal Processing Systems, 2001 IEEE Workshop; Page(s): 349 - 360.

Ramesh Karri, Kaijie Wu, Piyush Mishra, Yongkook Kim; "Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers"; June 2001; Proceedings of the 38th conference on Design automation.

The following Non-Patent Literatures pertain to different speed test results obtained by substituting row bytes of shifted columns based on Rijndael cipher algorithm; and different speed test results using different key sizes.

a. http://groups-beta.google.com/group/comp.lang.forth - May 28 2001, 1:59 pm by Jabari Zakiya "Advanced Encryption Standard (AES) 2ND PART"; Google Group.

b. http://groups-beta.google.com/group/comp.lang.forth - May 28 2001, 1:48 pm by Jabari Zakiya; "Advanced Encryption Standard (AES) 2-PARTS"; Google Group.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
June 21, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100